JLARC RFP #2018-001

Answers to questions submitted by potential bidders during RFP process

*Current as of *April 16, 2018*. Additional questions will be added (if asked) and answered until the RFP submission deadline.

**NOTE: This version includes a changed answer to Q6.

Q1: Does JLARC have preferences for whether the review of policies and procedures, or the testing of technical vulnerabilities, should be the primary emphasis?

A1: Given that we are policy generalists and not IT security experts, we will welcome proposals that articulate the merits of emphasizing either policy and procedural reviews or technical testing. The proposal evaluation team will seek to choose a vendor that will be able to provide as much useful information as possible for a reasonable price.

Q2: Does JLARC have preferences for the how the testing of technical vulnerabilities should be performed?

A2: Given that we are policy generalists and not IT security experts, we will welcome proposals that suggest the most appropriate way(s) to test technical vulnerabilities and those that clearly articulate the relative merits of those different ways of testing.

Q3: Are you looking for basic vulnerability scans of VERIS infrastructure, penetration testing, or both?

A3: Given that we are policy generalists and not IT security experts, we will welcome proposals that suggest the most appropriate way(s) to test technical vulnerabilities of infrastructure. These may certainly include basic vulnerability scans, penetration testing, or other methods of which we may not be aware. Our proposal evaluation team will seek to weigh the benefits of these types of activities against what they will cost, in an attempt to choose a vendor that will be able to provide as much useful information as possible for a reasonable price.

Q4: For the actual VERIS application are you looking for application penetration testing, application vulnerability scanning, both, or none as part of this review?

A4: Our primary focus will need to be the VERIS application itself. However, we are aware that hardware certainly matters as well for security. So we will welcome proposals that suggest the most appropriate way to understand the application and its infrastructure. The proposal

evaluation team will then seek to choose a vendor that will be able to provide as much useful information as possible for a reasonable price.

Q5: For the VERIS application, assuming that application is in-scope for this review, do you want the selected vendor to test with authenticated credentials? If so, how many roles will the selected vendor need to test the application with (i.e. admin access, manager, basic user access, etc)?

A5: The VERIS application is the primary focus so is certainly in-scope. We will welcome proposals that articulate the merits of vendors testing with authenticated credentials vs. other forms of testing. The proposal evaluation team will then seek to choose a vendor that will be able to provide as much useful information as possible for a reasonable price.

Q6: For the VERIS application, assuming that the application is in-scope for this review, is there a lower environment (i.e. QA, staging, etc) where the application testing can be conducted to ensure that any outage would cause minimal business impact?

A6: We understand from the Department of Elections that VERIS does have a “non-production environment.” *However, we also understand it is very difficult to provide outside entities access to this environment. This may mean that practically speaking, there is not an available non-production environment for the purposes of this engagement (different answer as of April 16).*

Q7: Are there any known budget caps or expectations on this?

A7: In terms of budget, we are using the RFP process to find a reasonable price.

Q8: We’re trying to understanding the technical testing requirements. The Task/Deliverables noted in sections 3-5 of the RFP mention "Testing of Technical Vulnerabilities." Which of the four options listed is required: (a) application vulnerability assessment of the web application, (b) internal server and network vulnerability assessment, (c) unassisted network and application penetration test, and/or (d) all of the above or some combination.

A8: We are policy generalists, so are really hoping that bidders will propose what they think makes the most sense. We would welcome a proposal that suggests a series of technical approaches (so any or all of your options 1 -4) and makes the case for those in consideration of the proposed pricing.

Q9: Approximately how many infrastructure components (servers, databases, etc) are supporting the VERIS application? The RFP says “databases” and “servers” which are plural so there is an implication that there is more than one database and server.

A9: It is our understanding that VERIS is currently using 21 servers (14 production, 3 sandbox, 2 testing, and 2 development). The Department of Elections has informed us that two testing servers will be turned off soon, and that several new production servers will be online in the near future.

Q10: We understand six bound proposals are to be delivered to you. Do these also need to be delivered by 2 PM on Thursday, April 19?

A10: It is our strong preference that we also get the hardcopies by the deadline.

Q11: What are the policies and procedures referenced as part of task 2, e.g., VITA security policy and standards, others?

A11: The most relevant policies and procedures would be those set for all state agencies by the Virginia Information Technologies Agency (VITA), and those used by the Department of Elections itself. We would welcome proposals that explain how these policies and procedures-(in addition to other non-Virginia state government standards) can be used to understand how secure VERIS is.

Q12: For section V. 3. Testing of technical vulnerabilities of VERIS – what does the scope of the testing entail? (a) penetration testing of known vulnerabilities, (b) vulnerability scanning of the system and addressing discovered vulnerabilities, (c) a complete security controls assessment as part of a certification and accreditation (C&A)/security assessment and authorization (SA&A) effort that will end in an authorization to operate (ATO). This would include an assessment of NIST SP 800-53 Management, Operation, and Technical controls.

A12: Given that we are policy generalists and not IT security experts, we will welcome proposals that suggest the most appropriate way(s) to test technical vulnerabilities of the VERIS application itself and associated infrastructure. These may certainly include penetration testing, vulnerability scanning, or a complete security controls assessment. Our proposal evaluation team will seek to weigh the benefits of these types of activities against what they will cost, in an attempt to choose a vendor that will be able to provide as much useful information as possible for a reasonable price.

Q13: What is the security categorization of VERIS? Low, Moderate, or High?

A13: Our preliminary interviews with state officials indicate that VERIS is an important system, but perhaps not among the state’s most important systems in terms of security. It is our understanding that the highest level of security categorization is reserved for state systems that, if compromised, could place people in immediate physical danger (e.g. state police systems or emergency response systems).

Q14: Does updated security documentation (e.g. System Security Plan (SSP), Contingency Plan, Incident Response Plan, etc.) exist for the VERIS system? If not, which ones will need to be developed?

A14: It is our understanding that the Department of Elections is working with the Virginia Information Technologies Agency to ensure documentation exists that addresses risk management and state audit standards.

Q15: Section VI . Pricing mentions that JLARC will only pay for satisfactorily-completed tasks and deliverables, and then mentions hourly rates. Is JLARC looking for Time & Material pricing or Fixed-Fee pricing?

A15: We are interested in a fixed-price structure through which we pay for the completed deliverables / tasks listed in the table in section V. In other words, we will not pay any additional fees or a certain amount based on how many hours the chosen contractor takes to complete the deliverables.

Q16: What is the budget allocation for this assessment?

A16: In terms of budget, we are using the RFP process to find a reasonable price.

Q17: Has JLARC ever performed a risk assessment of VERIS? If so, can that be shared with the winning vendor?

A17: JLARC has never done a risk assessment of VERIS. Several other organizations, though, have. These include the U.S. Department of Homeland Security, the Virginia National Guard, and the Virginia Information Technologies Agency. JLARC will work with the Department of Elections to facilitate the winning vendor being able to learn the results of these assessments.

Q18: Does JLARC anticipate the selected vendor to perform an assessment of the general registar's workstations? If so, how many?

A18: Our primary focus is the state-owned VERIS application and state-owned infrastructure. However, understanding that each general registrar has workstations that use the VERIS application, we would more than welcome proposals that suggest the most appropriate way to fully understand the security of the application and all infrastructure and hardware (e.g. randomly sampling workstations at selected registrars' offices with JLARC's assistance). The proposal evaluation team will seek to choose a vendor that will be able to provide as much useful information as possible for a reasonable price.

Q19: Are the communications closets, network closets and/or data centers in each of the school districts built out with the same set of standards?

A19: School divisions in Virginia have a fair degree of autonomy to manage their information technology resources based on local needs and resources. It is highly likely there is substantial variation in the information technology infrastructure used across--and even within--school divisions.

Q20: Does JLARC wish to have a penetration test and vulnerability scan, or just a vulnerability scan?

A20: Given that we are policy generalists and not IT security experts, we will welcome proposals that suggest the most appropriate way(s) to test technical vulnerabilities of infrastructure. These may certainly include vulnerability scans, penetration testing, or other methods of which we may not be aware. Our proposal evaluation team will seek to weigh the benefits of these types of activities against what they will cost, in an attempt to choose a vendor that will be able to provide as much useful information as possible for a reasonable price.

Q21: If vulnerability scanning is to be performed, will the vendor be granted privileged user rights to reduce false positives or will scan have to be performed by a general user account?

A21: JLARC will work with the Department of Elections to provide the winning vendor with access rights that are necessary to perform the work.

Q22: Does JLARC have centralized management responsibility and authority over the VERIS system? Will the winning vendor have access to the VERIS system at the state data center maintained by VITA?

A22: The Department of Elections administers the VERIS application, and it is hosted on infrastructure operated by the Virginia Information Technologies Agency. JLARC has no authority over VERIS, though JLARC has been tasked with reviewing the system in its capacity as the legislature's oversight agency for a one-time assessment. JLARC will work with the Department of Elections to provide the winning vendor access as appropriate to perform the work.

Q23: How many devices are within scope if a vulnerability scan/penetration is desired?

A23: We are policy generalists, so hope that bidders will propose what they think makes the most sense in terms of how many devices. We would welcome a proposal that suggests potential technical approaches and makes the case for those in consideration of the proposed pricing. It is our understanding that VERIS is currently using 21 servers.

Q24: Are there any time of day restrictions for conducting technical testing such as penetration testing and vulnerability scanning?

A24: JLARC will work with the Department of Elections to determine whether there are time-of-day restrictions for testing.

Q25: Is the security assessment being driven by any compliance or regulatory requirements? Does JLARC have a preferred security framework to conduct this engagement?

A25: The most relevant policies and procedures would be those set for all state agencies by the Virginia Information Technologies Agency and those used by the Department of Elections itself. We would welcome proposals that explain how these policies and procedures (in addition to other non-Virginia state government standards) can be used to understand how secure VERIS is.

Q26: Can documentation including security policies and procedures be reviewed at the vendor's offices?

A26: JLARC will work with the Department of Elections to ensure the winning vendor can access security policies and procedures at the vendor's offices if that is most efficient.

Q27: Does JLARC have a required format in which the final assessment report needs to be delivered in?

A27: JLARC will work with the winning vendor to determine a mutually agreeable format for the final assessment. As long as the assessment includes the key points and describes them clearly, JLARC will largely defer to the winning vendor in terms of format.

Q28: Does the Commonwealth of Virginia adhere to a recognized security standard, such as NIST SP 800-53, CIS Controls, ISO 27001, etc.?

A28: At this point in our study, we do not know how the Virginia Information Technologies Agency and Department of Elections standards relate to other standards, such as NIST or ISO. We welcome proposals that articulate the merits of applying at least key parts of multiple standards. The proposal evaluation team will then seek to choose a vendor that will be able to provide as much useful information as possible for a reasonable price.

Q29: Can the security policy and procedure review be done remotely?

A29: JLARC will work with the Department of Elections to ensure the winning vendor can access security policies and procedures at the vendor's offices if that is most efficient.

Q30: Does the Commonwealth provide tools such as Nessus, Nexpose, etc., or is the vendor expected to supply these?
A30: It is our expectation that a vendor will have access to needed tools, or propose an approach for them to gain access as necessary.

Q31: How many databases are in scope? How many workstations are in scope? Are the operating system and other supporting infrastructure in scope? How many external interfaces and Internet Protocol addresses/sub-addresses (IPs) are in scope?
A31: We are policy generalists, so hope that bidders will propose what they think makes the most sense in terms of how many devices. We would welcome a proposal that suggests potential technical approaches and makes the case for those in consideration of the proposed pricing. It is our understanding that VERIS is currently using 21 servers.

Q32: Is there a vulnerability management program in place for VERIS? If so, will the vendor have access to resulting scan reports, Plans of Action and Milestones (POA&Ms), etc.?
A32: The Department of Elections is currently working to improve the security of the VERIS system. JLARC will work with the Department of Elections to facilitate access by the selected vendor to any / all relevant programs, reports, etc.

Q33: Are there any special requirements for the personnel conducting the review? (i.e. security clearances)
A33: It is our understanding that the VERIS system contains some personally sensitive information, but not information requiring security clearances to access.

Q34: Any constraints that would prevent consultants from performing interviews and evidence collection? (i.e. Restricted physical access to facilities)
A34: The Department of Elections is in a state office building. JLARC staff will work with the selected vendor to facilitate access to employees and to the Department of Elections office as necessary.

Q35: Will we also be able to interview/interact with VITA personnel for the purpose of gathering information around the application?
A35: JLARC staff will work with the selected vendor to facilitate interviews or other interactions with VITA staff.

Q36: Approximately how many databases does VERIS send information into?
A36: It is our understanding that VERIS is currently using 21 servers (14 production, 3 sandbox, 2 testing, and 2 development). The Department of Elections has informed us that two testing servers will be turned off soon, and that several new production servers will be online in the near future.

Q37: Any special instructions around the format of the deliverable?
A37: JLARC will work with the winning vendor to determine a mutually agreeable format for deliverables. As long as the deliverables include the key points and describe them clearly, JLARC will largely defer to the winning vendor in terms of format.

Q38: Is there a contract vehicle JLARC prefers to use for pricing, i.e. GSA?
A38: We have no strong preferences for any particular contract vehicle.

Q39: Would JLARC be amenable to invoicing on a monthly basis for T&E incurred and by milestone for deliverables?
A39: The selected vendor may invoice monthly, but we are interested in a fixed-price structure through which we pay for the completed deliverables / tasks listed in the table in section V. In other words, we will not pay any additional fees or a certain amount based on how many hours the chosen contractor takes to complete the deliverables.

Q40: Provide the following information for each VERIS application server in scope: Approximately how many static pages? How many dynamic pages that accept user input or query a database are included?

A40: According to the Virginia Department of Elections, VERIS has approximately: 100 dynamic content pages (the actual count is probably closer to 200 individual pages, but this count is based off of the menu items); 15 static content pages; and 20 main functional areas (e.g. - voter registration, petition processing, absentee, etc.).

Q41: What technology and programing languages were used to build the application?
A41: VERIS was originally built by Quest Information Systems for the state of Indiana. The application is currently in the C#.NET 2.0 format and runs on SQL Server 2014 databases.

Q42: Approximately how many total live hosts (e.g., servers, workstations, network devices) are expected to be assessed?

A42: VERIS is currently using 21 servers (14 production, 3 sandbox, 2 testing, and 2 development). The Department of Elections has informed us that two testing servers will be turned off soon, and that several new production servers will be online in the near future.

The VERIS system includes several desktop applications:

- Desktop Application for General Registrars (DAGR) - Enables the GRs to view the alpha roster, generate PDF pollbooks and delivers the state electronic pollbook software and data.
- Public Application for Record Examination (PARE) - Enables the GRs to setup a computer for locally registered voters to view the registered voter list as required by law.
- Voter Photo Identification (VoPhoId) - Enables the GRs to capture and submit the photo and signature of a voter to ELECT so we can print their voter photo identification card.

The VERIS system also includes several public web applications:

- Election Night Reporting (ENR) - Used by the public to view results
- Citizen Portal (OVR) - Used by citizens to view their record and apply to register to vote or to apply to vote absentee
- Client Services - Used by staff to manage the voter data sales process
- APIs - Used by third-party groups and DMV to submit electronic voter registration record

Q43: Approximate number of user input pages in the application (e.g., 1-5, 6-9, 10+):

A43: 100 dynamic content pages (the actual count is probably closer to 200 individual pages, but this count is based off of the menu items); 15 static content pages; and 20 main functional areas (e.g. - voter registration, petition processing, absentee, etc.).

Q44: Number of user roles/privilege levels (e.g., admin, power user, customer) in the application:

A44: Several administrative roles in the Department of Elections and Virginia Information Technologies Agency. Several hundred users / customers across each of the state's 133 general registrar offices.

Q45: Does the application include an administrative interface?

A45: Yes

Q46: What regulatory standard does the Commonwealth of Virginia follow with respect to cybersecurity? NIST SP 800-53? ISO27001? Some other standard?
A46: At this point in our study, we do not know how the Virginia Information Technologies Agency and Department of Elections standards relate to other standards, such as NIST or ISO. We welcome proposals that articulate the merits of applying at least key parts of multiple standards. The proposal evaluation team will then seek to choose a vendor that will be able to provide as much useful information as possible for a reasonable price.

Q47: How many total users are authorized to access the VERIS System?
A47: There are several administrative users at in the Department of Elections and Virginia Information Technologies Agency. There are several hundred other authorized users across the state's 133 general registrar offices.

Q48: Are there plans to do any assessment of the physical security, internal and/or external vulnerability scans of the remote access locations?
A48: Given that we are policy generalists and not IT security experts, we will welcome proposals that suggest the most appropriate way(s) to test VERIS' vulnerabilities. These may certainly include vulnerability scans, or perhaps assessments of physical security as well. Our proposal evaluation team will seek to weigh the benefits of these types of activities against what they will cost, in an attempt to choose a vendor that will be able to provide as much useful information as possible for a reasonable price.

Q49: What cybersecurity training do the users receive prior to authorization to access the VERIS System?

A49: We understand that general registrars (and potentially some of their staff) had the opportunity to attend "Cyber Security Awareness Training" at the 2017 Annual Training Event. We do not believe, though, that this training was mandatory and it is unclear at this point how many VERIS users attended the training. It is also unclear whether this represents the full extent of cybersecurity training.

Q50: If we are allowed to use the QA environment, will this test environment be accessible from the Internet or will it require that we physically connect behind a firewall, requiring us to be on-site at some data center? In the past in such circumstances we have either had to handle it one of two ways:

- The client allows the testing from the Internet, sometimes by providing a VPN connection with appropriate credentials. Sometimes the client will configure special firewall rules to route our traffic to the hosts to be tested. We can provide our external IP addresses if this is possible.
- If the client can't provide an Internet-accessible connection, we must physically test from inside their QA environment. We don't have a problem either way, we would just like to know, if possible, which method we would be asked to use.

A50: Given that we are policy generalists and not IT security experts, we will welcome proposals that suggest the most appropriate way(s) to test VERIS' vulnerabilities. We will work with the Department of Elections to facilitate access as appropriate depending on the chosen vendor's recommendation. Our proposal evaluation team will seek to weigh the benefits of these types of activities against what they will cost, in an attempt to choose a vendor that will be able to provide as much useful information as possible for a reasonable price.

Q51: Does JLARC want a fixed price or a price broken down by hourly rates?

A51: We are interested in a fixed-price structure through which we pay for the completed deliverables / tasks listed in the table in section V. In other words, we will not pay any additional fees or a certain amount based on how many hours the chosen contractor takes to complete the deliverables.